PB-01 – Ochrona danych osobowych pacjentów (zgodnie z RODO)

1. Kod i nazwa

PB-01 – Procedura ochrony danych osobowych pacjentów i współpracowników Medweed

2. Cel procedury

Celem procedury jest zapewnienie zgodnego z prawem, bezpiecznego i przejrzystego przetwarzania danych osobowych pacjentów, lekarzy, współpracowników oraz kontrahentów w ramach działalności **WEKK Sp. z o.o. (Medweed)**.
Procedura określa praktyczne zasady stosowania RODO w codziennej pracy personelu medycznego, administracyjnego i technicznego.

3. Zakres stosowania

Procedura obejmuje:

- dane pacjentów (w tym dane medyczne),
- dane lekarzy i współpracowników,
- dane kontrahentów (np. aptek, dostawców IT),
- systemy: **Aurero, PayU, WordPress, poczta Zoho medweed.pl, LHhosting,**
- dokumentację papierową (*Załącznik nr 1 – zgoda pacjenta*).

4. Odpowiedzialność

- **Administrator danych** – WEKK Sp. z o.o., reprezentowana przez Prezesa Zarządu **Konrada Welenca**.
- **Koordynator medyczny** – nadzór nad zgodnością przetwarzania danych pacjentów i wniosków o dostęp.
- **Administrator IT (Karol Salamądry)** – bezpieczeństwo systemów i integracji technicznych.
- **Lekarze i współpracownicy** – obowiązek stosowania zasad minimalizacji i poufności.

5. Zasady ogólne przetwarzania danych

5.1. Zasady wynikające z art. 5 RODO

Dane muszą być:
a) **przetwarzane zgodnie z prawem**, rzetelnie i w sposób przejrzysty;
b) **zbierane w konkretnych i uzasadnionych celach** (np. świadczenie usług medycznych);
c) **ograniczone do niezbędnego minimum**;
d) **prawidłowe i aktualne**;
e) **przechowywane nie dłużej niż to konieczne** (co do zasady 20 lat dla dokumentacji medycznej);
f) **chronione przed nieuprawnionym dostępem**;
g) **udokumentowane** – każda czynność przetwarzania musi mieć podstawę i cel.

6. Opis postępowania

Krok 1. Pozyskanie danych

- Dane pacjentów pozyskuje się wyłącznie:
    - przez formularz rejestracyjny online (WordPress / Aurero),
    - podczas wizyty stacjonarnej (Załącznik nr 1),
    - poprzez kontakt telefoniczny lub mailowy (rejestracja).
- Dane zbierane są w zakresie niezbędnym do wykonania usługi: imię, nazwisko, PESEL, kontakt, dane medyczne.
- Pacjent przed pierwszą wizytą musi podpisać lub zaakceptować **zgodę na przetwarzanie danych osobowych i leczenie - załącznik nr 1 do regulaminu organizacyjnego.**

Krok 2. Przechowywanie i dostęp

- Dane przechowywane są wyłącznie w systemie **Aurero**, który spełnia wymogi bezpieczeństwa ISO 27001 i RODO.
- Fizyczne zgody pacjentów (Załącznik nr 1) przechowywane są w gabinetach lekarskich (patrz procedura PA-10).
- Dostęp do danych ma wyłącznie personel Medweed z indywidualnym loginem.
- Dane nie są zapisywane lokalnie na prywatnych komputerach ani w przeglądarkach.

Krok 3. Udostępnianie danych

- Dane mogą być udostępniane wyłącznie:
    - pacjentowi lub osobie upoważnionej,
    - organom państwowym na podstawie przepisów prawa,
    - podmiotom przetwarzającym (np. Aurero, PayU, hosting, firmy IT) – wyłącznie na podstawie **umowy powierzenia danych (DPA)**.

- Zabronione jest przekazywanie danych innym placówkom medycznym, jeśli pacjent nie wyraził zgody lub nie istnieje inna podstawa prawna.

Krok 4. Przechowywanie i usuwanie danych

- Dane pacjentów przechowuje się przez **20 lat od daty ostatniego wpisu**, a w przypadku zgonu – **30 lat**.
- Dane pracowników i współpracowników – przez okres zatrudnienia + 5 lat archiwizacji.
- Dane z formularzy kontaktowych online są automatycznie usuwane po 90 dniach, jeśli nie doszło do wizyty.
- Wniosek o usunięcie danych (prawo do bycia zapomnianym) rozpatruje Prezes Zarządu w terminie 30 dni, jeśli nie koliduje to z przepisami o dokumentacji medycznej.

Krok 5. Środki bezpieczeństwa

- Każdy komputer lub urządzenie służbowe musi mieć:
  - aktualny system i oprogramowanie,
  - hasło lub biometryczne zabezpieczenie,
  - wygaszacz ekranu po 5 minutach bezczynności.
- Zabronione jest:
  - używanie prywatnych nośników USB,
  - przesyłanie danych pacjentów przez prywatne konta e-mail lub komunikatory,
- Wszelkie podejrzenia naruszenia bezpieczeństwa danych zgłasza się natychmiast wg procedury **PB-03 – Incydent RODO**.

Krok 6. Edukacja i poufność

- Każdy lekarz i współpracownik przed uzyskaniem dostępu do danych musi podpisać **Oświadczenie o zapoznaniu się z procedurami ochrony danych** (PA-04 / DPA).
- Administrator IT i osoby z dostępem technicznym (np. Karol Salamądry) podpisują dodatkowo **umowę powierzenia danych**.
- Szkolenia RODO przeprowadzane są co najmniej raz na 12 miesięcy lub po każdej zmianie przepisów.

7. Dokumentacja i zapisy

- Rejestr czynności przetwarzania danych osobowych (RODO log).

- Umowy powierzenia danych (Aurero, PayU, hosting, IT).
- Oświadczenia o poufności i szkoleniach.
- Rejestr incydentów bezpieczeństwa (PB-03).

8. Uwagi / ryzyka

- Naruszenie zasad PB-01 może skutkować sankcjami administracyjnymi (do 20 mln EUR wg RODO) i karnymi.
- Utrata nośnika z danymi lub dostęp nieautoryzowany traktowane są jako incydent.
- Dane pacjentów nie mogą być wykorzystywane w celach marketingowych bez ich wyraźnej zgody.
- Wszelkie działania z danymi muszą być możliwe do udokumentowania (zasada rozliczalności).

9. Załączniki

- **Wzór Oświadczenia o zapoznaniu się z procedurami ochrony danych (RODO)**
- **Rejestr czynności przetwarzania danych osobowych – wzór**
- **Instrukcja minimalnych środków technicznych bezpieczeństwa (PB-05)**

PB-02 – Zarządzanie uprawnieniami dostępu do systemów informatycznych

1. Kod i nazwa

PB-02 – Procedura nadawania, weryfikowania i odbierania uprawnień dostępu do systemów informatycznych WEKK Sp. z o.o. (Medweed)

2. Cel procedury

Celem procedury jest zapewnienie bezpieczeństwa informacji poprzez kontrolę dostępu do systemów teleinformatycznych, w których przetwarzane są dane osobowe pacjentów i współpracowników, oraz zapobieganie nieautoryzowanemu dostępowi, utracie lub modyfikacji danych.

3. Zakres stosowania

Procedura dotyczy wszystkich systemów wykorzystywanych w Medweed, w szczególności:

- **Aurero** – elektroniczna dokumentacja medyczna,
- **PayU / mBank** – obsługa płatności,
- **WordPress / WooCommerce** – strona internetowa i sklep,
- **Serwery, hosting, poczta firmowa medweed.pl**,
- **Narzędzia integracyjne,**
- **Dostęp administracyjny do systemów (Karol Salamądry / IT)**.

4. Odpowiedzialność

- **Administrator Danych (Prezes Zarządu – Konrad Welenc)** – zatwierdzanie uprawnień i nadzór strategiczny.
- **Koordynator Medyczny** – zgłaszanie zmian kadrowych i kontrola dostępu lekarzy.
- **Każdy użytkownik** – obowiązek zachowania poufności loginów i haseł oraz natychmiastowego zgłaszania incydentów.

5. Opis postępowania

Krok 1. Nadanie dostępu

1. Dostęp do systemów nadaje się wyłącznie osobom, które posiadają ważną umowę współpracy lub formalne polecenie Prezesa Zarządu.
2. Administrator IT nadaje dostęp na podstawie polecenia (pisemnego, mailowego lub przez komunikator służbowy).
3. Każdy użytkownik otrzymuje:
    - indywidualny login,
    - tymczasowe hasło (do zmiany przy pierwszym logowaniu),
    - informację o zakresie dostępu.
4. Nadanie dostępu jest rejestrowane w **Rejestrze dostępów** zawierającym: imię, nazwisko, system, datę nadania, osobę zatwierdzającą.

Krok 2. Zmiana uprawnień

1. Każda zmiana w zakresie dostępu (np. dodanie modułu, konta e-mail, dostępu administracyjnego) wymaga zgody Prezesa Zarządu lub Koordynatora Medycznego.

2. Zabrania się samodzielnego tworzenia kont użytkowników lub duplikowania dostępów.

Krok 3. Odbieranie dostępu

1. W dniu zakończenia współpracy lub zawieszenia aktywności użytkownika administrator IT:
    - natychmiast blokuje konta użytkownika,
    - resetuje lub usuwa hasła,
    - usuwa dostęp do integracji, baz danych i chmury,
    - aktualizuje Rejestr dostępów.
2. W przypadku podejrzenia naruszenia bezpieczeństwa – konto użytkownika blokuje się **natychmiast**, niezależnie od statusu umowy.

Krok 4. Weryfikacja okresowa

1. Raz w miesiącu administrator IT dokonuje przeglądu aktywnych kont w systemach: Aurero, WordPress, PayU, poczta.
2. Co 6 miesięcy sporządza raport bezpieczeństwa dostępu i przekazuje go Prezesowi Zarządu.
3. Konta nieużywane dłużej niż 30 dni podlegają dezaktywacji.

Krok 5. Zasady bezpieczeństwa kont

- Hasła muszą:
    - mieć minimum 10 znaków, zawierać cyfry, duże i małe litery, znak specjalny,
    - być zmieniane co 90 dni,
    - nie mogą być współdzielone ani zapisywane w widocznym miejscu.
- Zabrania się:
    - logowania z nieautoryzowanych urządzeń,
    - korzystania z kont innych użytkowników,
    - używania prywatnych skrzynek e-mail do komunikacji służbowej.

6. Dokumentacja i zapisy

- **Rejestr dostępów do systemów Medweed** (utrzymywany przez Administratora IT),
- **Raport z miesięcznych przeglądów aktywnych kont**,

- **Raport półroczny z audytu dostępów**,
- **Zgłoszenia incydentów bezpieczeństwa (PB-03)**.

7. Uwagi / ryzyka

- Brak kontroli nad dostępami może prowadzić do naruszenia RODO.
- Każdy dostęp do danych pacjentów przez osobę nieuprawnioną stanowi incydent RODO.
- Nieusunięcie kont po zakończeniu współpracy to ryzyko poważnej kary administracyjnej.

PB-03 – Postępowanie w przypadku incydentu bezpieczeństwa lub naruszenia danych osobowych (RODO)

1) Kod i nazwa

PB-03 – Procedura reagowania na incydenty bezpieczeństwa i naruszenia ochrony danych (RODO)

2) Cel

Zapewnić szybkie wykrycie, ograniczenie skutków i zgodne z prawem (RODO) obsłużenie:

- incydentów **poufności** (ujawnienie/nieuprawniony dostęp),
- **integralności** (modyfikacja/uszkodzenie danych),
- **dostępności** (utrata/awaria),
  dotyczących danych pacjentów, współpracowników i systemów Medweed.

3) Zakres

Wszyscy lekarze, personel, podwykonawcy (w tym **Karol Salamądry – Admin IT**), wszystkie systemy: **Aurero, poczta medweed.pl, WordPress/hosting, PayU, chmura/integracje** oraz dokument papierowy **Załącznik nr 1**.

4) Role i odpowiedzialność

- **Administrator Danych (AD):** Prezes Zarządu – decyzje prawne, zgłoszenie do **UODO** w 72 h, komunikacja zewnętrzna.
- **Koordynator medyczny:** przyjęcie zgłoszenia, ewidencja, koordynacja działań na danych medycznych.

- **Admin IT (Karol Salamądry):** izolacja/naprawa techniczna, kopie dowodowe, przywracanie usług.
- **Zgłaszający (każdy użytkownik): natychmiast** zgłasza incydent – nie naprawia „na własną rękę”.

5) Definicja incydentu (przykłady)

- E-mail z dokumentacją/ereceptą wysłany do **złego adresata**.
- Utrata/kradzież urządzenia z dostępem do skrzynki lub systemów.
- Błąd uprawnień (ktoś widzi cudzych pacjentów w Aurero).
- Ransomware/phishing, podejrzenie wycieku z hostingu/WordPressa.
- Zgubienie **Załącznika nr 1** (papier).
- Dłuższa awaria Aurero (niedostępność dokumentacji).

6) Tryb natychmiastowy (T+0–2 h)

1. **Zgłoś od razu** do AD + Koordynatora + Admina IT (mail/telefon).
   Treść: *co, kiedy, gdzie, kogo dotyczy, jakie dane, ilu osób, systemy, podjęte kroki*.
2. **Izoluj źródło** (Admin IT): wylogowanie, blokada konta, odłączenie urządzenia/sieci, zmiana haseł, wstrzymanie integracji.
3. **Zabezpiecz dowody:** zrzuty ekranu, logi, nagłówki e-mail, numery IP, czas zdarzenia, kopia plików zsumowana (hash).

Zakaz samodzielnego kasowania śladów i korespondencji.

7) Analiza ryzyka (T+2–12 h)

Koordynator + Admin IT przygotowują dla AD krótką kartę ryzyka:

- **Jakie dane?** (identyfikacyjne vs. medyczne)
- **Skala osób?** [1–10 / 11–99 / 100+]
- **Poufność naruszona?** (TAK/NIE)
- **Dostępność/integralność naruszona?** (TAK/NIE)
- **Prawdopodobieństwo szkody** (niskie/średnie/wysokie)
- **Potencjalne skutki** (stygmatyzacja/strata finansowa/utrata dostępu do leczenia, itp.)

Kryterium zgłoszenia do UODO (art. 33 RODO): ryzyko dla praw i wolności **> niskie** ⇒ zgłosić w **72 h**.
Kryterium powiadomienia osób (art. 34): ryzyko **wysokie** ⇒ niezwłocznie poinformować osoby, prostym językiem + zalecenia.

8) Decyzje i działania (T+12–24 h)

AD podejmuje decyzję:

- **A. Rejestracja bez zgłoszenia do UODO** (ryzyko niskie) **lub**
- **B. Zgłoszenie do UODO** (ryzyko > niskie)
    - ewentualnie **zawiadomienie osób**, jeśli ryzyko wysokie.

Działania techniczne: reset haseł, wycofanie tokenów, aktualizacje, łatki, weryfikacja uprawnień (PB-02/PA-08).

9) Zawiadomienia – wzory treści

9.1. Zgłoszenie do UODO (72 h, ePUAP/e-mail urzędowy)

- Charakter naruszenia (co się stało, kiedy).
- Kategorie i przybliżona liczba osób/danych.
- Konsekwencje (potencjalne).
- Podjęte środki (izolacja, zmiana haseł, itp.).
- Dane kontaktowe AD.
- Plan działań naprawczych i prewencji.

9.2. Powiadomienie osób (niezwłocznie, jeśli ryzyko wysokie)

- Co się wydarzyło i kiedy (prosto).
- Jakie dane mogły zostać ujawnione.
- Co już zrobiliśmy.
- **Co powinien zrobić pacjent** (np. ignorować podejrzane telefony, zmiana hasła do IKP, kontakt pod adresem …).
- Dane kontaktowe do osoby wyjaśniającej w Medweed.

10) Scenariusze szybkie (checklisty)

A. E-mail do złego adresata

1. Odwołaj wiadomość/wyślij prośbę o usunięcie. 2) Zmień tematykę kanałów (przestań korespondować). 3) Oceń zakres ujawnienia. 4) Decyzja AD (UODO/osoby). 5) Wdrożenie „double-check" adresów.

B. Zgubiony/lub skradziony telefon/laptop

1. Zdalna blokada/wipe. 2) Reset haseł. 3) Zgłoszenie na Policję (kradzież). 4) Ocena ryzyka (dostęp do poczty/Aurero?). 5) Decyzje dot. zgłoszeń.

C. Phishing/ransomware

1. Izolacja stacji/segmentu. 2) Analiza IOCs/logów. 3) Przywrócenie z kopii. 4) Reset uprawnień/kluczy. 5) Ocena obowiązku zgłoszeń.

D. Awaria Aurero (dostępność)

1. Zgłoszenie do Aurero/monitoring statusu. 2) Praca na procedurze zastępczej (przyjmowanie pacjentów bez EDM, notatki tymczasowe bez danych wrażliwych). 3) Uzupełnienie EDM ≤ 24 h po przywróceniu.

E. Utrata Załącznika nr 1 (papier)

1. Przeszukaj/odtwórz zdarzenie. 2) Zgłoszenie do AD jako incydent RODO. 3) W razie potrzeby ponowne podpisanie od pacjenta. 4) Decyzja o zgłoszeniach.

11) Zamknięcie incydentu (T+24–72 h)

- Raport końcowy (1–2 strony): przyczyna, skala, decyzje, zgłoszenia, dowody, działania naprawcze, wnioski.
- Wpis do **Rejestru naruszeń RODO** (data, typ, system, liczba osób, decyzja o zgłoszeniu, referencje do dowodów).
- **Retencja dowodów:** min. **5 lat** (logi, korespondencja, snapshoty konfiguracji).

12) Prewencja po incydencie

- Szkolenie „lessons learned" (15 min na odprawie).
- Modyfikacja procedur (PB-01/PB-02/PA-08) i konfiguracji (MFA, DLP, DMARC, ograniczenia eksportu).
- Miesięczna kontrola wdrożenia poprawek (checklist).

13) Dokumentacja i rejestry

- **Rejestr naruszeń RODO** (excel/airtable – tylko dla AD/Koordynatora).

- **Repo dowodów** (katalog z dostępem tylko AD/IT).
- Zgłoszenia do **UODO** / powiadomienia osób (kopie).
- Raporty końcowe i plan działań.

14) Kontakt i eskalacja (drabinka)

1. **AD (Prezes):** decyzje prawne i zgłoszenia.
2. **Koordynator medyczny:** dane medyczne, komunikacja wewnętrzna.
3. **Admin IT (Karol Salamądry):** izolacja, logi, odzysk.
4. **Zgłaszający:** pierwsza informacja i współpraca przy ustaleniach.

Załączniki (wzory – krótkie)

- **PB-03/Z1** – karta incydentu (jedna strona, punkty 6–9).
- **PB-03/Z2** – zgłoszenie do UODO (szablon pól).
- **PB-03/Z3** – powiadomienie osoby, której dane dotyczą.
- **PB-03/Z4** – rejestr naruszeń (kolumny: data, typ, system, osoby, decyzja, nr sprawy, uwagi).

PB-03/Z1 – KARTA ZGŁOSZENIA INCYDENTU BEZPIECZEŃSTWA / NARUSZENIA DANYCH

Numer sprawy: _____ Data i godzina zgłoszenia: //_____ :
Zgłaszający (imię i nazwisko / rola): _____
Kontakt zgłaszającego (tel./e-mail): _____
Miejsce/system: ☐ Aurero ☐ Poczta medweed.pl ☐ WordPress/hosting ☐ PayU ☐ Chmura/ integracje ☐ Inne: _____

1. Opis zdarzenia (co się stało, kiedy, jak wykryto):

2. Kategorie danych i szacunkowa liczba osób, których dotyczy:
☐ Dane identyfikacyjne ☐ Dane kontaktowe ☐ Dane medyczne ☐ Dane finansowe
Szacunkowa liczba osób: _____

3. Wpływ na: ☐ Poufność ☐ Integralność ☐ Dostępność
4. Podjęte natychmiastowe działania (izolacja, blokady, zmiana haseł itp.):

5. Dowody zabezpieczone (logi, zrzuty, pliki – lokalizacja):

6. Eskalacja (kogo powiadomiono, kiedy):
AD (Prezes): _____ godz. **:** Koordynator medyczny: _____ godz. **:**
Admin IT: _____ godz. **:**

Podpis zgłaszającego: _____ Data: //_____

PB-03/Z2 – SZABLON ZGŁOSZENIA NARUSZENIA DO UODO (72 h)

Administrator danych: WEKK Sp. z o.o. (Medweed), ul. Michała Kajki 10–12, 10-547 Olsztyn
Osoba kontaktowa (AD): _____ (tel. _____, e-mail _____)

1. Charakter naruszenia (opis, data/godzina, system, przyczyna jeśli znana):

2. Kategorie i przybliżona liczba osób oraz rekordów danych:
Kategorie osób (pacjenci/współpracownicy/inne): _____
Liczba osób: _____ Liczba rekordów/dokumentów: _____
Kategorie danych: ☐ identyfikacyjne ☐ kontaktowe ☐ medyczne ☐ finansowe ☐ inne: _____

3. Możliwe konsekwencje naruszenia dla osób, których dane dotyczą:

4. Środki podjęte lub proponowane w celu zaradzenia naruszeniu i zminimalizowania skutków:

5. Informacje dodatkowe (np. czy osoby zostały powiadomione, kiedy i jak):

Załączniki (dowody, logi, korespondencja): _____

Data i podpis AD: //_____ _____

PB-03/Z3 – POWIADOMIENIE OSOBY, KTÓREJ DANE DOTYCZĄ (wysokie ryzyko)

Nadawca: WEKK Sp. z o.o. (Medweed), ul. Michała Kajki 10–12, 10-547 Olsztyn
Data: //_____
Dotyczy: Informacja o naruszeniu ochrony Pani/Pana danych osobowych

Szanowna Pani/Szanowny Panie,
w dniu //_____ doszło do naruszenia ochrony danych w systemie _____. Zdarzenie polegało

na:
[krótki, zrozumiały opis – co się stało].

Jakie dane mogły zostać ujawnione/objęte naruszeniem:

Co zrobiliśmy niezwłocznie po wykryciu zdarzenia:

Co mogą Państwo zrobić, aby się zabezpieczyć (praktyczne kroki):
— np. zmiana hasła do [IKP/portalu], ostrożność wobec nieznanych połączeń i e-maili, itp.

Kontakt do wyjaśnień:
Imię i nazwisko: _____ (WEKK Sp. z o.o.)
Telefon: _____ E-mail: _____

Przepraszamy za zaistniałą sytuację. Podejmujemy działania, by zapobiec podobnym incydentom w przyszłości.

Z poważaniem,
Administrator Danych – WEKK Sp. z o.o. (Medweed)
Podpis: _____

PB-03/Z4 – REJESTR NARUSZEŃ OCHRONY DANYCH (RODO)

Forma: arkusz (Excel/Sheets/Airtable) – kolumny jak poniżej.
Dostęp: wyłącznie AD, Koordynator medyczny, Admin IT.

Nr	Data/godz. wyk	Zgłaszający	System/obszar	Typ incydentu (poufność/	Kategorie danych	Szac. licz b	Krótki opis	Działania natychmiastowe	Decyzja AD (UODO/	Data zgłoszenia	Czy osoby powiadomione	Lokalizacja dowodó	Status (otw./zamk.)	Data zamknięcia	Uwagi/lessons learne

Instrukcje ewidencji:

- Każdy wiersz = jedno zdarzenie (numeracja roczna: 1/2025, 2/2025…).
- „Lokalizacja dowodów” → ścieżka do katalogu incydentu (logi, zrzuty, kopie, hash).
- „Decyzja AD” → *Zgłoszenie do UODO: TAK/NIE* + uzasadnienie (1–2 zdania).
- Rejestr przechowywać min. **5 lat**.

PB-04 – Polityka haseł i uwierzytelniania wieloskładnikowego (MFA)

1) Kod i nazwa

PB-04 – Procedura zarządzania hasłami oraz MFA w systemach WEKK Sp. z o.o. (Medweed)

2) Cel

Zapewnienie wysokiego poziomu bezpieczeństwa dostępu do danych i systemów Medweed poprzez jednolite zasady tworzenia, przechowywania i rotacji haseł oraz obowiązkowe stosowanie MFA wszędzie tam, gdzie to możliwe.

3) Zakres

Dotyczy wszystkich użytkowników (lekarze, administracja, podwykonawcy) oraz wszystkich systemów: **Aurero, poczta medweed.pl, WordPress/hosting, PayU/mBank, chmura i integracje (n8n/CRM), urządzenia końcowe**.

4) Role i odpowiedzialność

- **Administrator Danych (AD / Prezes)** – nadzór, egzekwowanie.
- **Każdy użytkownik** – bezwzględne przestrzeganie PB-04.

5) Zasady ogólne (must-have)

1. **MFA obowiązkowe**: dla Aurero, poczty firmowej, panelu hostingu/WordPress, chmury, PayU/mBank i wszelkich kont administracyjnych.
2. **Jeden użytkownik = jedno konto.** Żadnych kont współdzielonych.
3. **Hasła nie są zapisywane** w przeglądarkach prywatnych ani notatnikach; dopuszczalny **menedżer haseł**
4. **Zakaz** używania tych samych haseł w wielu systemach.
5. **Brak** przekazywania haseł innym osobom (również „na chwilę").

6) Wymagania dla haseł

- **Długość:** minimum **12 znaków** (kontrola administracyjna).
- **Składnia:** małe + wielkie litery + cyfry + znak specjalny.
- **Reużycie:** zakaz użycia ostatnich **5** haseł.
- **Ważność:** rotacja co **90 dni** (kontrolowana automatycznie, gdzie możliwe).
- **Blokada konta:** po 5 nieudanych logowaniach (czasowa – 15 min).

- **Frazy zabronione:** imię, nazwisko, „medweed”, PESEL, numer telefonu, „Password123!” itp.
- **Hasła tymczasowe:** ważne maks. 24 h, wymuszenie zmiany przy pierwszym logowaniu.

7) MFA – implementacja

- **Preferowane metody:** aplikacja TOTP (np. Microsoft/Google Authenticator), **FIDO2/U2F** (klucz sprzętowy).
- **Dopuszczalne awaryjnie:** SMS (tylko gdy TOTP/U2F niemożliwe).
- **Kody zapasowe:** każdy użytkownik generuje i **przechowuje offline** (wydruk/sejf).
- **Reset MFA:** wyłącznie przez Admina IT po **weryfikacji tożsamości** (telefon + potwierdzenie e-mail z konta firmowego). Zdarzenie odnotować w dzienniku zmian.

8) Urządzenia i sesje

- Ekran blokowany po **5 min** bezczynności, odblokowanie: hasło/biometria.
- Laptopy/telefony służbowe zabezpieczone hasłem/biometrią; szyfrowanie dysku włączone.
- **Automatyczne wylogowanie** z paneli po 15 min bezczynności (jeśli dostępne).
- Brak logowania do systemów Medweed z urządzeń niezabezpieczonych lub współdzielonych prywatnie.

9) Procedury operacyjne

9.1. Nadanie konta

- Admin IT tworzy konto → wysyła **hasło tymczasowe** oddzielnym kanałem.
- Użytkownik ustawia własne hasło + włącza **MFA** przy pierwszym logowaniu.
- Admin IT potwierdza w **Rejestrze dostępów** (PB-02/PA-08).

9.2. Zmiana/utrata hasła

- Użytkownik resetuje hasło w systemie; jeśli brak dostępu – kontakt z Adminem IT.
- Po resetach krytycznych (poczta, hosting, finanse) **wymuszone MFA rebind**.

9.3. Zakończenie współpracy / czasowe zawieszenie

- Natychmiastowa **blokada kont**, unieważnienie tokenów i kluczy API, rotacja haseł administracyjnych powiązanych (PB-02/PA-08).

- Wpis do Raportu z dezaktywacji.

9.4. Incydent bezpieczeństwa (phishing/wyciek)

- **Natychmiastowa** zmiana wszystkich haseł + rotacja tokenów, wymuszenie MFA.
- Zgłoszenie zgodnie z **PB-03**.
- Weryfikacja logów i sesji aktywnych.

10) Wyjątki i tryb awaryjny

- Wyjątki (np. brak MFA z przyczyn technicznych) zatwierdza **AD na piśmie** z okresem ważności **≤ 14 dni**.
- Hasła awaryjne (sealed envelope) dopuszczalne tylko dla kont serwerowych „break glass", przechowywane w sejfie; każde użycie → wpis do dziennika wraz z powodem i podpisem.

11) Naruszenia i sankcje

- Udostępnienie hasła, wyłączanie MFA lub obchodzenie zasad = **poważne naruszenie** procedur bezpieczeństwa; skutkuje konsekwencjami służbowymi i może być kwalifikowane jako incydent RODO (PB-03).

PB-05 – Minimalne środki techniczne bezpieczeństwa (stacje robocze, poczta, serwisy)

1) Kod i nazwa

PB-05 – Procedura minimalnych zabezpieczeń technicznych IT w WEKK Sp. z o.o. (Medweed)

2) Cel

Ustanowienie **minimalnych, obowiązkowych** zabezpieczeń dla urządzeń, poczty i usług on-line Medweed, tak aby ograniczyć ryzyko incydentów RODO i utraty danych.

3) Zakres

- Urządzenia: laptopy, komputery, telefony używane do pracy (także BYOD, jeśli dopuszczone).
- Systemy/usługi: **Aurero**, poczta **medweed.pl**, hosting/WordPress, PayU/mBank, chmura/integracje (n8n/CRM).
- Użytkownicy: lekarze, administracja, podwykonawcy (w tym Admin IT).

4) Role i odpowiedzialność

- **Administrator Danych (AD/Prezes)** – zatwierdza standard.
- **Każdy użytkownik** – stosowanie zasad i natychmiastowe zgłaszanie niezgodności.

5) Wymogi dla stacji roboczych (Windows/macOS/Linux)

5.1. Dostęp i blokada

- Ekran automatycznie blokowany po **5 min** bezczynności.
- Logowanie: hasło/biometria **+** PIN/TouchID/Windows Hello.
- Zakaz kont współdzielonych.

5.2. Szyfrowanie dysku – obowiązkowe

- Windows: **BitLocker** (TPM, PIN przy starcie – jeśli możliwe).
- macOS: **FileVault** (recovery key zapisany u Admina IT).
- Nośniki USB: domyślnie **zablokowane**; wyjątki – tylko szyfrowane.

5.3. Aktualizacje i oprogramowanie

- Auto-aktualizacje **systemu i przeglądarek** – włączone.
- Blokada uruchamiania makr Office z niezaufanych źródeł.
- Oprogramowanie tylko z **legalnych repozytoriów**.

5.4. Ochrona endpointów

- Antywirus/EDR **aktywny** (Defender/ATP, CrowdStrike/inna – jedna platforma).
- Zapora hosta **włączona** (in/out, blokada przy sieciach publicznych).
- Skany pełne co **14 dni**; alerty do Admina IT.

5.5. Przeglądarki

- Menedżer haseł firmowy lub systemowy; zakaz zapisywania haseł do krytycznych paneli w przeglądarce bez głównego hasła.

- Blokada wtyczek niezatwierdzonych; auto-update rozszerzeń.

6) Poczta firmowa i domena (medweed.pl)

6.1. Uwierzytelnianie

- **MFA obowiązkowe** dla wszystkich skrzynek.
- Reset dostępu — tylko przez Admina IT po weryfikacji tożsamości.

6.2. Zabezpieczenia domeny

- **SPF**: rekord ograniczający do zaakceptowanych nadawców.
- **DKIM**: podpisy włączone dla wszystkich wychodzących.
- **DMARC**:
  - faza 1: `p=quarantine; pct=100; rua=…; ruf=…`
  - po 30 dniach bez fałszywych trafień → **faza 2**: `p=reject`.
- **MTA-STS** i **TLS-RPT** – włączone (wymuszanie TLS i raporty).

6.3. Ochrona anty-phishing

- Filtracja załączników (blok *.exe, *.js, archiwa hasłowane – kwarantanna).
- Ban listy domen typosquatting (medwed, med-weed itp.).
- Szkolenie „rozpoznaj phishing” co 12 miesięcy.

7) Serwisy www i integracje (WordPress/hosting/n8n/CRM)

7.1. WordPress/hosting

- Aktualizacje **core + wtyczki + motywy** – min. co tydzień; wtyczki tylko z repo WP.
- Minimalizacja wtyczek; kasowanie nieużywanych.
- **WAF** aplikacyjny włączony (Cloudflare/hosting).
- Loginy adminów: unikalne, **MFA**; zakaz konta „admin”.
- Kopie zapasowe **codziennie**, retencja min. **14 dni**, kopia off-site.

7.2. Klucze i API

- Klucze API przechowywane **poza kodem** (secrets manager/zmienne środowiskowe).
- Rotacja kluczy **co 90 dni** lub natychmiast po incydencie.

- Uprawnienia **najmniejszego zakresu** (least privilege).

8) Sieci i łączność

- Preferowane połączenia **VPN** do paneli administracyjnych.
- Sieci Wi-Fi: WPA2-Enterprise/WPA3; hasła sieciowe rotowane **co 90 dni**.
- Goście: osobny SSID **bez** dostępu do zasobów firmowych.
- Zdalny pulpit/RDP: zakaz z Internetu; tylko przez VPN + MFA.

9) Urządzenia mobilne (BYOD/firmowe)

- PIN/biometria obowiązkowe; auto-blokada **≤ 2 min**.
- Szyfrowanie pamięci telefonu włączone; kopie w chmurze prywatnej **wyłączone** dla danych służbowych.
- E-mail firmowy w kontenerze (MDM/Work Profile jeśli możliwe).
- Zgubienie/kradzież → **zdalny wipe** i zgłoszenie wg PB-03.

10) Kopie zapasowe i odtwarzanie (Backup/DR)

- Krytyczne systemy (poczta, WWW, CRM/integracje): backup **codzienny**, retencja **≥ 14 dni**, jedna kopia **off-site/immutability**.
- Test odtworzenia **co 6 miesięcy** (raport z testu do AD).
- Backupy szyfrowane, dostęp ograniczony (MFA, logowanie zdarzeń).

11) Logowanie i monitoring

- Logi: logowania, nieudane próby, zmiany uprawnień, aktualizacje, użycie kluczy API.
- Retencja logów **≥ 180 dni**; dostęp tylko Admin IT/AD.
- Alerty e-mail dla: 5× failed login, wyłączenie MFA, instalacja nowej wtyczki WP, modyfikacja DNS.

12) Zakazane praktyki

- Praca na **publicznych** komputerach/wi-fi bez VPN.

- Przesyłanie danych pacjentów prywatnym mailem/komunikatorami.
- Przechowywanie danych pacjentów na nieszyfrowanych pendrive’ach.
- Wtyczki/tematy „nulled”, pirackie oprogramowanie.

13) Dokumentacja i zapisy

- Rejestr urządzeń (model, właściciel, szyfrowanie, AV, ostatnia aktualizacja).
- Raport miesięczny zabezpieczeń (patching, AV, backup, DMARC).
- Protokoły testów DR.
- Rejestr wyjątków (czasowych odstępstw) – z terminem i podpisem AD.

14) Wyjątki

Wyjątki techniczne dopuszczalne **wyłącznie** na piśmie przez AD, na okres **≤ 30 dni**, z planem usunięcia niezgodności.

Załączniki (1 str. – do wdrożenia)

PB-05/A – Checklista stacji roboczej

- Szyfrowanie (BitLocker/FileVault)
- Auto-lock 5 min
- AV/EDR aktywny, ostatni skan ≤14 dni
- Auto-update system/przeglądarek
- Zapora włączona
- Brak niezatwierdzonych wtyczek
- VPN skonfigurowany (jeśli zdalnie)

PB-05/B – Checklista poczty i domeny

- MFA dla wszystkich kont
- SPF poprawny
- DKIM aktywny
- DMARC `p=quarantine` → po 30 dniach `p=reject`
- TLS wymuszony (MTA-STS/TLS-RPT)

- Filtry anty-phishing

PB-05/C – Checklista WordPress/hosting

- Core/wtyczki/motywy aktualne
- MFA adminów, brak konta „admin”
- WAF aktywny
- Backup codzienny, retencja 14 dni, test odtwarzania
- Klucze/API poza kodem, rotacja 90 dni

Podpisy i zatwierdzenie

Opracował:	Konrad Kołodziejski	10.10.2025	Konrad Kołodziejski .....
Zatwierdził:	Konrad Kołodziejski Konrad Welenc	10.10.2025	Konrad Welenc ..... Konrad Kołodziejski

Stanowisko: Członkowie Zarządu WEKK Sp. z o.o.